UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/735,985	12/15/2003	Man-Pyo Hong	587-34	4178

28249 7590 02/20/2009

DILWORTH & BARRESE, LLP
333 EARLE OVINGTON BLVD.
SUITE 702
UNIONDALE, NY 11553

EXAMINER	
HOANG, DANIEL L	
ART UNIT	**PAPER NUMBER**
2436	
MAIL DATE	**DELIVERY MODE**
02/20/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/735,985	HONG ET AL.	
	Examiner	Art Unit	
	DANIEL L. HOANG	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 November 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Detailed Action

Response to Arguments

Applicant's arguments filed 11/17/08 have been fully considered but they are not persuasive. Applicants' amendments are treated below.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-9 are rejected under 35 U.S.C. 102(e) as being anticipated by Ji (US Patent No. 6,272,641).

As per claim 1, Ji teaches:

A method of detecting malicious scripts using code insertion technique, comprising the step of:

checking values related to each sentence belonging to call sequences by using method call sequence detection based on rules including matching rules and relation rules,

[see col 5, lines 10-15, wherein the applet is conventionally interpreted by the web browser and its instructions are executed. The instructions are viewed as analogous to the claimed "sentences"] the matching rules and relation rules are treated below.

wherein said matching rules comprise general script sentences and further include a variable string; and

[see col. 5, lines 16-21, wherein the static (pre-run time) scanning is performed on the applet by the scanner, if an instruction that calls an insecure function is found, a first instruction sequence is inserted..]

Applicant's specification cites that a condition of the matching rule is satisfied if a sentence having the same pattern as that described in the [conditional statement] is present. The Ji reference seeks to determine whether an insecure function is called, which is viewed as analogous to the claimed matching rule as defined by applicant.

wherein said relation rules are comprised of condition phrases and action phrases and wherein the action phrases are executed when the conditions of the condition phrase are satisfied, wherein said condition phrases are comprised of at least one condition expression for checking whether one of: (a) a rule has already been satisfied, (b) specific variable values of two rules are equal to each other or (c) one of the specific variables is include in the other value; and

[see col. 5, lines 21-42, wherein the pre-filter checks to see of the particular instruction is allowed and a post-filter function is called.]

[See col. 5, lines 45-67, for an example of pseudo code of the instrumentation process which is viewed as analogous to the claimed "relation rules comprised of condition phrases and action phrases.]

wherein the checking step comprises the steps of:

inserting a self-detection routine (malicious behavior detection routine) call sentence before and after a method call sentence of an original script; and

[see col. 5, lines 21-26]

detecting the malicious codes during execution of the script through a self-detection routine inserted into the original script.

[see col. 5, lines 38-43]

As per claim 2, Ji teaches:

The method according to claim 1, wherein the self-detection routine call sentence is generated by a script transformer which transforms an original script including method call sentences into a script capable of continuously performing self-detection during execution through the method call sequence based on the detection rules and the self-detection routine,

[see fig. 2, element 26, scanner]

wherein the self-detection routine is composed of sentences for storing parameters and return values and calling a detection engine, said sentences being inserted before and after the method call sentence when the method call sentence matches with contents described in the matching rule, and wherein the self-detection routine includes a rule-based detection engine for executing for executing the relation rule related to a relevant matching rule when a method corresponding to the matching rule is called and detecting the presence of malicious behavior of the method call sequence, and methods for causing the parameters and return values of the method call sentence satisfying the matching rule to be stored into a buffer usable by the detection engine.

[see fig. 2]

As per claim 3, Ji teaches:

The method according to claim 1, further comprising selecting one rule as a higher level rule, representative of all relation rules in a set of relation rules.

[see co.. 5, line 55, wherein the if function precedes a later if function on col. 6, line 13. The first if function representing a higher level rule than any preceding if function]

As per claim 4, Ji teaches:

The method according to claim 1, further comprising upon satisfying the conditions of the condition phrases, generating an instance of a relation rule and thereafter checking at least one higher level rule.

[see col. 5, lines 21-24, wherein an instruction must first call an insecure function before a first instruction sequence is run]

As per claim 5, Ji teaches:

The method according to claim 4, wherein a higher level rule is a rule with a relevant rule included in its own condition expression.

[see col. 5, line 55]

As per claim 6, Ji teaches:

The method according to claim 1, further comprising loading matching rules and relation rules from a rule description file.

[see col. 6, lines 34-38

As per claim 7, Ji teaches:

The method according to claim 6, further comprising generating a corresponding method from each matching rule.

[see col. 5, lines 50-53, wherein each function has its own method]

As per claim 8, Ji teaches:

The method according to claim 6, further comprising generating a corresponding method from each relation rule

[see col. 5, lines 50-53, wherein each function has its own method]

As per claim 9, Ji teaches:

The method according to claim 1, further comprising initializing each self-detection routine (malicious behavior detection routine) call sentence located before and after each of said method call sentences of an original script, prior to performing said continuous detection.

[see col. 5, lines 21-26 and col. 5, line 53]

POINTS OF CONTACT

*. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulaney Street
Alexandria, VA 22314

*. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Daniel L. Hoang/
Examiner, Art Unit 2436

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436